

SENTINEL ESSENTIALS

*Gain a bird's eye view across your enterprise
with SIEM for a modern world*

Description

See and stop threats before they cause harm with Open Systems Sentinel Essentials

Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response. Get an overview of Azure Sentinel along with insights on active threats to your Microsoft 365 cloud and on-premises environments with an Azure Sentinel Workshop. This package of work can be used as a pre-enabler for our Managed Detection & response service

Deliverables in 3 phases

- Workshops, design, and preparation
- Deployment
- Pilot/POC completion – MDR next steps

WORKSHOPS, DESIGN AND PREPARATION

Highlights

-  Understand the features and benefits of Azure Sentinel
-  Better understand, prioritize, and mitigate potential threat vectors
-  Create a defined deployment roadmap based on your environment and goals
-  Develop joint plans and next steps

DEPLOYMENT

Highlights

- Configure and enable Microsoft Sentinel, with applicable connectors
- Discover threats and demonstrate how to automate responses
- Understand how to mitigate threats by showing how Microsoft 365 and Azure security products can help mitigate and protect against threats that are found

PILOT/POC COMPLETION — MDR NEXT STEPS

- Summary of POC/Pilot (Q/A)
- Knowledge transfer to customer's security team
- Next step discussion on MDR

Open Systems is a premier Microsoft security partner and has access to Microsoft investment funding (if applicable) which can help co-fund this specific package of work. Please speak to an Open Systems Sales representative for more information and to see if your organization is eligible.